UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/620,176	07/20/2000	Baber Amin	1565.023US1	3893

21186 7590 07/26/2007

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/620,176
Filing Date: July 20, 2000
Appellant(s): AMIN ET AL.

Joseph P Mehrle
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 9 March 2007 appealing from the Office action mailed 2 November 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,490,679	TUMBLIN ET AL	12-2002
6,304,974	SAMAR	10-2001

SSL-Talk List FAQ Secure Sockets Layer Discussion List FAQ v1.1.1, 21 November 1999

Novell Netware Connection Enhanced NetWare 5 "What's Enhanced in NetWare 5", May 1998

Microsoft Security Advisor SSL Specific WSAIoctl Controls, 1999

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-2, 4, 6-9, 12, 14-18, and 20 are rejected under 35 U.S.C. 102(e) as being anticipated by Tumblin et al US Patent No. 6,490,679.

With regards to claims 1 and 7, Tumblin teaches directly receiving application data, from an application, at an upper connection layer of a transport protocol stack (Tumblin, column 8 lines 19-28), wherein the application data is received from the application using a connection specific application programming interface (API) desired for communication by the application and which is not associated with security (Tumblin,

column 8 lines 19-28, NSIM creates new connection), passing the application data from the upper connection layer to a security layer from within the transport protocol stack and unbeknownst to the application (Tumblin, column 8 lines 19-21 and Figure 7 Item 210), encrypting the application data within the security layer (Tumblin, column 8 lines 45-53), passing the encrypted application data from the security layer (Tumblin, Figure 7 Item 290) to a lower connection layer of the transport protocol stack (Tumblin, column 9 lines 45-49 and Figure 7), and sending encrypted application data from a lower connection layer out a network connection (Tumblin, column 9 lines 45-49 and Figure 7). The application disclosed by Tumblin is not required to perform security handshakes in order to send encrypted application data over the network (Tumblin, column 9 lines 50-53 and column 8 lines 10-11), the connection layer supports at least one network transport protocol and the security layer is not specific to the transport protocol (Tumblin, column 8 lines 19-22).

With regards to claims 2 and 16, Tumblin teaches receiving encrypted application data at the lower connection which came in at the network connection (Tumblin, column 9 lines 38-49, Figures 2 and 7), decrypting the application data within the security layer (Tumblin, column 9 lines 39-45), passing the decrypted application data from the upper connection layer to the application (Tumblin, column 8 lines 19-20, column 9 lines 39-49, Figures 2 and 7) without requiring that the application perform a security handshake (Tumblin, column 9 lines 50-53 and column 8 lines 10-11).

With regards to claims 8-9 and 17, Tumblin teaches connection layers comprising code for performing a WinSock network transport protocol (Tumblin, column 8 lines 19-22) and a Secure Socket Layer Session (Tumblin, column 7 lines 16-20).

With regards to claim 12, Tumblin teaches the security layer and at least one of the connection layers identifying a particular application and its cryptographic properties (Tumblin, column 8 lines 19-27 and 45-53).

With regards to claims 4 and 14, Tumblin teaches a means for establishing a secure connection using a specified handshake mode (Tumblin, column 7 lines 16-20 and column 8 lines 19-22).

With regards to claim 15, Tumblin teaches a legacy application that performs security handshakes (Tumblin, column 6 lines 15-24) and a security module that supports a secure connection to the legacy application (Tumblin, column 6 lines 22-24).

With regards to claim 18, Tumblin teaches the receiving of the encrypted application data at the lower connection layer using a transport model (Tumblin, column 8 lines 10-22).

With regards to claim 20, Tumblin teaches a secure network communications protocol stack interface which is callable from at least the lower connection layer (Tumblin, column 9 lines 38-60).

Claims 3 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tumblin et al US Patent No. 6,490,679 in view of SSL-Talk List FAQ Secure Sockets Layer Discussion List FAQ v1.1.1 ("SSL-Talk List FAQ).

With regards to claim 3, Tumblin, as described above, fails to teach the lower connection layer establishing a connection with a handshake mode that is at least one of an interactive mode and a blind-root accept mode. The SSL-Talk List FAQ teaches the use of an interactive mode when establishing a connection with a handshake (SSL-Talk List FAQ, Section 5.3). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the FAQ's suggested interactive mode with Tumblin's system because it offers the advantage of allowing a user to override a failed attempt to authentication a server (SSL-Talk List FAQ, Section 5.3).

With regards to claim 10, Tumblin as modified fails to teach the connection layer performing transport layer security sessions. The SSL-Talk List FAQ teaches the inclusion of Transport Layer Security Protocols within secure communication systems (SSL-Talk List FAQ, Section 6.2.1).

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tumblin et al US Patent No. 6,490,679 in view of Samar US Patent No. 6,304,974. Tumblin, as described above, fails to teach the changing of a list of trusted roots for a secure connection. Samar teaches the changing of a list of trusted roots (Samar, column 7 line 53 – column 8 line 7). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Samar's method of updating lists of trusted roots with Tumblin's system because it offers the advantage of allowing a user to avoid a particular certificate authority if the user does not have confidence in their entity authentication (Samar, column 2 lines 4-13).

Claims 11 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tumblin et al US Patent No. 6,490,679 in view Novell NetWare Connection Enhanced NetWare 5 "What's Enhanced in NetWare 5."

With regards to claims 11 and 19, Tumblin, as described above, fails to teach an application comprising code for providing lightweight directory access protocol services. "What's Enhanced in NetWare 5" teaches the inclusion of applications providing LDAP services using a transport protocol in the form of a Novell transport ("What's Enhanced in NetWare 5", Section "Lightweight Directory Access Protocol LDAP support"). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the enhancements defined by "What's Enhanced in NetWare 5" because it offers the advantage of allowing users to easily access X.500 based directories such as NDS.

Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tumblin et al US Patent No. 6,490,679 in view Microsoft Security Advisor SSL Specific WSAIoctl Controls ("MS SSL Advisor"). Tumblin, as described above, fails to teach the identifying of a function as a call back function. The MS SSL Advisor teaches the use of a call back function (MS SSL Advisor, Page 1/15, Paragraph 2). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize the MS SSL Advisor's call back function because it offers the advantage of allowing the service

provider to access security information from the application as it considers necessary (MS SSL Advisor, Page 1/15, Paragraph 2).

(10) Response to Argument

Applicant asserts that the Tumblin reference fails to teach or suggest the following limitations:

> "directly receiving application data, from an application, at an upper connection layer...received from the application using a connection specific application programming interface...and which is not associated with security; passing the application data from the upper connection layer to a security layer...unbeknownst to the application...the application is not required to perform security handshakes...and the security layer is not specific to that transport protocol."

Applicant's main argument is that the Tumblin reference fails to teach, "an application that benefits from security and that is unaware of that security and is not pre-configured to support the security" (Appeal Brief, page 12). Examiner respectfully disagrees.

I. Defining "Security Unaware"

In arguing the deficiencies of Tumblin, Applicant has not identified a definition for an application that is security unaware that is supported by the specification. Applicant

merely asserts that the Tumblin reference fails to define an application that benefits from security and that is unaware of that security and is not pre-configured to support the security. Thus, it is important to look to the specification to give some guidance as to what is meant by "security unaware."

The specification defines the invention as providing "applications with a virtual "hands free" environment for establishing and maintaining secure Internet connections using SSL, TLS, or other security layer, without regard to network configuration or low level protocol considerations" (Specification, page 7 lines 7-10). Further, the specification provides that "a given application 200 is unaware of and free from interaction with any detailed aspect of the infrastructure for secure transport. The applications 200 will receive and send their data 204 in clear form (i.e., not encrypted) and the applications 200 do not have to worry about SSL/TLS related functions such as SSL/TLS handshake, encryption, and decryption." Hence, the applications of the instant invention have all of their security related functionality offloaded to other network elements freeing the applications from having to deal with security issues. The applications will act as if no security is necessary and other portions of the system step in to provide security. This definition of security unaware compares favorably with Tumblin's security non-extensible application that Examiner has relied upon to teach the claimed limitation. As is described in greater detail below, Tumblin's security non-extensible application acts free from interaction with any detailed aspect of the infrastructure for security. Instead, Tumblin's security non-extensible application is unaware that the security proceedings are commencing because all security functions

have been offloaded (Tumblin, column 8 lines 28-40, NSIM and SIM provide all authentication and authorization) and because the security non-extensible application does not recognize a security services API (Tumblin, column 3 lines 40-47).

II. Tumblin anticipates all of the limitations of claims 1, 7, and 16

Applicant argues that Tumblin fails to teach "directly receiving application data, from an application, at an upper connection layer...received from the application using a connection specific application programming interface...and which is not associated with security; passing the application data from the upper connection layer to a security layer...unbeknownst to the application...the application is not required to perform security handshakes...and the security layer is not specific to that transport protocol." Examiner respectfully disagrees.

Tumblin teaches directly receiving application data (Tumblin, column 8 lines 19-28, client program attempts to access data or services on a server), from an application (Tumblin, column 8 lines 19-28, client program), at an upper connection layer (Tumblin, column 8 lines 14-28, network API - Winsock connect function). Tumblin teaches this limitation by disclosing a client application that attempts to send data to a server. The client makes a connection request (Winsock connect function) to the network API (Tumblin, column 8 lines 14-17, network API 190). The Winsock connect function is a portion of the network API (application programming interface) which is found in an upper connection layer (Application layer).

Tumblin further teaches the application data being received from the application using a connection specific application-programming interface (Tumblin, column 8 lines 19-28, Winsock connect function). Tumblin teaches this limitation by teaching the client using the Winsock connection function which is a portion of the network API.

Tumblin further teaches that the application is not associated with security (Tumblin, column 8 lines 19-28, Winsock connect function, request is intercepted by NSIM which creates new connection). Tumblin teaches this limitation by disclosing that the client application is security non-extensible (Tumblin, column 10 lines 10-14). Tumblin defines security non-extensible as one that may not have any built in security and does not recognize a security services API (Tumblin, column 3 lines 40-47). Thus, Tumblin's security non-extensible client application is not associated with security. Instead, Tumblin's security non-extensible client application makes a generic connection request to the network API (Tumblin, column 8 lines 19-28, Winsock connect function). The client NSIM then intercepts the client application requests (Tumblin, column 8 lines 20-28). Once the client NSIM intercepts the connection requests of the client application, the client NSIM will then take care of security procedures by requesting that the Security Integration Module (SIM) open a new session, authenticate the client application (Tumblin, column 8 lines 25-32, NSIM calls OpenSession in the SIM API), and make SKI security service calls (Tumblin, column 5 lines 47-51). Thus, the client application attempts to open a new connection by using a generic Winsock Connect function call and the NSIM and SIM provide security without any assistance from the client application.

Tumblin further teaches passing the application data from the upper connection layer to a security layer (Tumblin, column 8 lines 19-21 and Figure 7 Item 210, data is passed from network API to NSIM to SIM), unbeknownst to the application (Tumblin, column 8 lines 19-28, requests are intercepted by NSIM). Tumblin teaches these limitations by teaching that the connection request is intercepted by the client NSIM (Tumblin, column 8 lines 20-26) and the client NSIM then passes the connection request to the Security Integration Module (SIM) (Tumblin, column 8 lines 25-32, NSIM calls OpenSession in the SIM API). The application is unaware that the security proceedings are commencing because the application does not recognize a security services API (Tumblin, column 3 lines 40-47). Instead, the application only recognizes the network API to which it interfaces (Tumblin, column 8 lines 14-18, see also Figure 7). Tumblin discloses this setup in Figure 7 where the client application (item 210) interfaces only with the network API (190).

Finally, Tumblin teaches that the application is not required to perform security handshakes (Tumblin, column 8 lines 29-57, security handshakes are commenced by SIM) and the security layer is not specific to that transport protocol (Tumblin, column 8 lines 19-28, column 3 lines 40-46, generic new network connection is requested using Winsock). Tumblin discloses these limitations by teaching that the NSIM and SIM combine to provide security features. For instance, the NSIM and SIM provide authentication and authorization (Tumblin, column 8 lines 28-40, authenticates user and authorizes requesting and receiving hosts). All security handshakes are performed by the NSIM and SIM because the application does not recognize a security services API

(Tumblin, column 3 lines 40-47). The client security non-extensible application makes a connection request, but does not make any requests for security handshakes or authentication. Security handshakes and authentication procedures are commenced by the NSIM and SIM.

III. Applicant's Arguments are not persuasive

Applicant argues that Tumblin's security non-extensible application is not security unaware because the security non-extensible application includes an API to interact with the NSIM and because the security non-extensible application is linked to the NSIM. Applicant's arguments fail because providing an API and linking with an application does not indicate that the application is security aware. As noted above, Tumblin's security non-extensible application does not recognize a security services API (Tumblin, column 3 lines 40-47). Instead, the security non-extensible application recognizes a standard network API allowing functions such as "Winsock connect" to be called in order to create a connection (Tumblin, column 8 lines 19-27). When the security non-extensible application makes a connection request, the NSIM intercepts and then commences security proceedings (Tumblin, column 8 lines 18-30). In other words, the NSIM provides a network API (Tumblin, column 5 lines 20-25, NSIM 290 and API 190) that is recognizable to an application that has no security awareness or built in

security (Tumblin, column 5 lines 43-51). The security non-extensible application makes no security calls to the NSIM (Tumblin, column 5 lines 47-51, does not receive such requests from security non-extensible client program). Instead, the NSIM takes care of all security proceedings without the application being aware because the application believes it is communicating through a standard Winsock connect function.

Tumblin discloses two types of applications: security extensible applications and security non-extensible applications (Tumblin, column 5 lines 14-24). The fact that the security non-extensible application is security unaware is clearly evident when compared against Tumblin's security extensible client application. Tumblin discloses a security extensible application that is linked to an application security interface module using the security services API (Tumblin, column 5 lines 14-20). Thus, the security extensible application must have embedded within it computer code that recognizes and interfaces with the security services API. This is a clear example of an application being security aware. The security extensible client is programmed to make function calls directly to a security services API. In contrast, the security non-extensible application makes calls to a network API and has the NSIM take over security proceedings. The security non-extensible application interfaces with a network API and the NSIM interfaces with the Security Integration Module (SIM) using the SIM API (Tumblin, column 5 lines 46-52). Thus, the NSIM is security aware because it is designed to interface with a security API in the form of the SIM API while the security non-extensible application is security unaware because it is designed to interface only with the network API.

The fact that Tumblin's security non-extensible application is security unaware is further evident when compared to the disclosure of the instant specification. As noted above, the instant specification defines the invention as providing "applications with a virtual "hands free" environment for establishing and maintaining secure Internet connections using SSL, TLS, or other security layer, without regard to network configuration or low level protocol considerations" (Specification, page 7 lines 7-10). Further, the specification provides that "a given application 200 is unaware of and free from interaction with any detailed aspect of the infrastructure for secure transport. Hence, applications act "unaware of and free from interaction with any detailed aspect of the infrastructure for secure transport." Tumblin's security non-extensible applications act free from interaction with any detailed aspect of the infrastructure for secure transport. The security non-extensible applications are free from any detailed aspect of the infrastructure for secure transport because the NSIM and the SIM take care of all security procedures such as making requests for SKI services (Tumblin, column 5 lines 45-51) or authentication and authorization procedures (Tumblin, column 8 lines 25-35). Thus, Tumblin's security non-extensible applications are security unaware in the same way that the instant invention's applications are security unaware.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Andrew Nalven

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron

Mathew Smithers

/Matthew Smithers/
Primary Examiner, AU 2137